AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An apparatus for managing access to a resource over a network, comprising:

a receiver that receives a request for access to the resource from a client device; and

a policy manager, coupled to the receiver, that performs actions, including:

downloading a component onto the client device, wherein the downloaded component inspects the client device to detect a configuration of the client device, including determining whether client-security software other than a virtual sandbox is active on the client device;

receiving from the downloaded component the configuration of the client device based on the inspection;

in response to the received request, applying, using the apparatus, a dynamic policy for the access based, in part, on the received configuration and the requested resource;

employing the virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

applying, using the apparatus, a restriction to the client device for access by the client device to the requested resource, the restriction based on the applied dynamic policy.

2. (Previously Presented) The apparatus of claim 1, wherein determining the configuration of the client device further comprises:

if the client device is configured to not download the component, then receiving the configuration of the client device through a browser residing on the client device.

3. (Previously Presented) The apparatus of claim 1, wherein the received configuration indicates whether the client device is operating as a kiosk.

4. (Original) The apparatus of claim 1, wherein determining the configuration of the client device further comprises determining information associated with the connection between the client device and the resource.

5. (Previously Presented) The apparatus of claim 1, wherein inspecting the client device to detect a configuration further comprises detecting if security software is installed on the client device and if security software is installed, inspecting the security software to detect if the security software is active or disabled.

6. (Original) The apparatus of claim 1, wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy.

7. (Original) The apparatus of claim 1, wherein the restriction includes at least one downloadable component.

8. (Previously Presented) The apparatus of claim 1, wherein the restriction intercepts a communication between the client device and the apparatus.

9. (Previously Presented) The apparatus of claim 1, wherein applying the restriction further comprises performing at least one of inhibiting a file save and inhibiting a file print.

10. (Currently Amended) A method implemented at a network device of managing access to a resource over a network, comprising:

receiving at the network device a request for access to the resource from a client device;

downloading a component onto the client device, wherein the downloaded component inspects the client device to detect a configuration of the client device, including determining what client security software is active on the client device;

receiving from the downloaded component the configuration of the client device based on the inspection;

in response to the received request, applying, using the network device, a dynamic policy for the access based, in part, on the received configuration and the requested resource;

employing the virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

applying, using the network device, a restriction to the client device for access by the client device to the requested resource, the restriction based on the applied dynamic policy.

11. (Original) The method of claim 10, further comprising in response to receiving the request for access to the resource, transmitting a downloadable component to the client device.

12. (Previously Presented) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating whether the client device is a laptop, personal computer, kiosk, or a mobile device.

13. (Previously Presented) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating at least one of one level of trust associated with the client device, a type of encryption enabled on the client device, a type of antivirus enabled on the client device, a security feature enabled on the client device, a browser type, an operating system configuration, a security certificate, and if a hacker tool is enabled on the client device.

14. (Previously Presented) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating a level of trust of the client device.

15. (Previously Presented) The method of claim 10, wherein receiving the configuration further comprises: receiving information indicating a characteristic of an enabled security application enabled.

16. (Original) The method of claim 10, wherein applying the restriction further comprises downloading a component to the client device.

17. (Previously Presented) The method of claim 10, wherein applying the restriction further comprises configuring a virtual sandbox to intercept a communication between the client device and the resource.

18. (Original) The method of claim 17, wherein intercepting the communication further comprises blocking a download of at least one file to the client device.

19. (Original) The method of claim 10, wherein applying the restriction further comprises:

if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command.

20. (Original) The method of claim 10, wherein applying the dynamic policy further comprises determining at least one of a connector, and an adaptor to enable the access to the resource.

21. (Original) The method of claim 10, wherein applying the dynamic policy further comprises restricting the access to the resource.

22. (Currently Amended) A network appliance for managing access to a resource over a network, comprising:

a transceiver for receiving a request for access to the resource from a client device; and

a processor that performs actions, including:

receiving at the network appliance the request for access from the client device;

downloading a component onto the client device, wherein the downloaded component inspects for a configuration of the client device including what client security software is active on the client device;

receiving from the downloaded component information about the configuration of the client device based on the inspection;

in response to the received request, applying, using the network appliance, a dynamic policy for the access based, in part, on the received configuration and the requested resource;

employing the virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

applying, using the network appliance, a restriction to the client device for access by the client device to the requested resource, wherein the restriction is configured based on the applied dynamic policy.

23. (Previously Presented) The network appliance of claim 22, wherein the processor performs further actions, comprising: in response to receiving the request for access to the resource, receiving additional information about the configuration of the client device through a query with a browser residing on the client device.

24. (Original) The network appliance of claim 22, wherein applying the restriction further comprises employing a virtual sandbox that is configured based on the applied dynamic policy.

25. (Previously Presented) The network appliance of claim 23, wherein determining the configuration of the client device further comprises:

if the client device is not configured to receive a downloadable component, receiving information about the configuration of the client device through a browser application residing within the client device.

26. (Original) The network appliance of claim 22, wherein applying the dynamic policy further comprises:

if the client device is configured to restricting a download of a component, restricting access to the resource.

27. (Original) The network appliance of claim 22, wherein applying the restriction further comprises:

if the client device is configured to restrict a download of a component, intercepting a communication between the client device and the requested resource to perform at least one of preventing an access to file, and restricting an action.

28. (Currently Amended) A computer readable storage medium that includes data and instructions, wherein the execution of the instructions on a computing device provides for managing access to a resource over a network by enabling actions, comprising:

receiving at the computing device a request for access to the resource from a client device;

downloading a component onto the client device, wherein the downloaded component inspects for a configuration of the client device including whether client security software is active on the client device;

receiving from the downloaded component information about the configuration of the client device based on the inspection;

in response to the received request, applying, using the computing device, a dynamic policy to the access based, in part, on the configuration of the client device and the requested resource;

employing the virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

applying, using the computing device, a restriction to the client device for access by the client device to the requested resource, the restriction based on the applied dynamic policy.

29. (Previously Presented) The computer readable storage medium of claim 28, wherein applying the restriction further comprises configuring a virtual sandbox to intercept a communication between the client device and the resource.

30. (Previously Presented) The computer readable storage medium of claim 28, wherein applying the restriction further comprises blocking a download of at least one file to the client device.

31. (Currently Amended) An apparatus for managing access to a resource over a network, comprising:

a transceiver that receives a request for access to the resource from a client device; and

a policy manager, coupled to the transceiver, that performs actions, including:

downloading a component onto the client device, wherein the downloaded component inspects the client device to detect a configuration of the client device including what client security software is active on the client device and whether a hacker tool is enabled on the client device;

receiving from the downloaded component information about the configuration of the client device based on the inspection, wherein the configuration includes at least an indication of a status of an security application residing on the client device including whether the application is active or disabled;

in response to the received request, applying, using the apparatus, a dynamic policy for the access based, in part, on the configuration and the requested resource;

employing a virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

restricting, using the apparatus, the client device for access by the client device to the requested resource, wherein the means for restricting is configured based, in part, on the applied dynamic policy.

32. (Currently Amended) A method implemented at a server device for managing access to a resource over a network, comprising:

receiving, at the server device, a request for access to the resource from a client device;

determining, using the server device, a level of security software enabled on the client device, including what antivirus software is active on the client device and whether a hacker tool is enabled on the client device;

in response to the received request, applying, using the server device, a dynamic policy to the access based, in part, on the determined level of security software enabled and the requested resource;

employing a virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

applying, using the server device, a restriction to the client device for access by the client device to the requested resource, the restriction based on the applied dynamic policy.

33. (Currently Amended) A method implemented at a network appliance for managing access to a resource over a network, comprising:

receiving at the network appliance a request for access to the resource from a client device;

determining if the client device is configured as a kiosk or a mobile device and whether client computing security software is active on the client device or whether a hacker tool is enabled on the client device;

employing a virtual sandbox at the client device to encrypt the resources using an encryption key that is separately stored on a remote server device; and

in response to the received request, applying, using the network appliance, a restriction to the client device for access by the client device to the requested resource, the restriction based on the determined configuration of the client device and the requested resource.

34. (Canceled)